UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/469,505	12/22/1999	ROBERT J. STONE	UUN99006	5044

25537 7590 07/13/2005

MCI, INC
1133 19TH STREET NW
WASHINGTON, DC 20036

EXAMINER	
LAFORGIA, CHRISTIAN A	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 07/13/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/469,505	STONE ET AL.	
	Examiner	Art Unit	
	Christian La Forgia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 April 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 28 April 2005 has been entered.

2. Claims 1-29 have been presented for examination.

Response to Arguments

3. Applicant's arguments with respect to claims 1-29 have been considered but are moot in view of the new ground(s) of rejection.

4. See further arguments that follow.

Claim Rejections

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

6. Claims 1-29 are rejected under 35 U.S.C. 102(a) as being anticipated by **CenterTrack: An IP Overlay Network for Tracking DoS Floods**, by Robert Stone.

7. As per claim 1, Stone teaches a method for tracking denial-of-service floods, the method comprising:

rerouting a DoS flood attack datagram to a tracking router, wherein the tracking router forms an overlay tracking network with respect to an egress edge router (Abstract, page 1, i.e. "CenterTrack is an overlay network, consisting of IP tunnels, that is used to selectively reroute interesting datagrams directly from edge routers to special tracking routers." "the datagrams can be examined, then dropped or forwarded to the appropriate egress point");

identifying, by the tracking router, an ingress edge router that forwarded the DoS flood attack datagram (Abstract, page 1, i.e. "the tracking routers can easily determine the ingress edge router by observing which tunnel the datagrams arrive on").

8. Regarding claim 2, Stone teaches executing security diagnostic functions (**3.3 Advantages and Disadvantages**, page 3, i.e. "hop-by-hop with overlay network: With this method, specialized diagnostic features are now only required only on edge routers and special-purpose tracking routers").

9. With regards to claims 3 and 15, Stone teaches wherein the security diagnostic functions comprise input debugging (page 2, first column, i.e. "*Input debugging* refers to the diagnostic features required to determine what adjacency originated a packet matching an attack signature on an individual router").

10. Regarding claims 4 and 16, Stone teaches wherein the overlay tracking network is within an autonomous system that is different from another autonomous system corresponding to the

ingress edge router and the egress edge router (**4.2 Routing Architecture**, page 4, i.e. "network as an external autonomous system using BGP").

11. With regards to claims 5, 11, and 17, Stone teaches providing routing information by the overlay tracking network to the ingress edge router and the egress edge router using an inter-administrative-domain routing/signaling protocol (**4.2 Routing Architecture**, page 4, i.e. "network as an external autonomous system using BGP").

12. Concerning claims 6, 12, and 18, Stone teaches wherein the inter-administrative-domain routing/signaling protocol is BGP (Border Gateway Protocol) (**4.2 Routing Architecture**, page 4, i.e. "network as an external autonomous system using BGP").

13. Regarding claims 7, 19, and 23, Stone teaches communicating between the edge routers and the tracking router via tunnels that are created over an unreliable datagram delivery service protocol (**5.2 Dynamic routing with Tunnels**, page 6).

14. Regarding claims 8, 20, and 24, Stone teaches communicating between the edge routers and the tracking router via virtual connections over a separate lower layer protocol (**4.4 Tracking Router Capabilities**, page 5, i.e. using IP tunnels).

15. Regarding claims 9, 21 and 25, Stone teaches communicating between the edge routers and the tracking router via physical connections (**5.4 Tunnel Termination**, pages 6-7).

16. Regarding claim 10, Stone teaches routing the DoS flood attack datagram from the ingress edge router to the tracking router, wherein the egress edge router has a static route to the victim (**6.1 Static Routes**, pages 7-8, i.e. "a static route for the victim, pointing through the egress edge adjacency").

17. Concerning claims 13 and 27, Stone teaches further comprising establishing another static route between the egress router and an external router associated with a victim node, the victim node receiving the DoS flood attack datagram (**6.1 Static Routes**, pages 7-8, i.e. "a static route for the victim, pointing through the tunnel to the egress edge router").

18. As per claim 14, Stone teaches a communication system for tracking denial-of-service (DoS) floods, the communication system comprising:

a plurality of edge routers including an ingress edge router and an egress edge router, each of the edge routers being configured to perform security diagnostic functions, in part, to identify a DoS flood attack datagram, wherein the ingress edge router is associated with a source of the DoS flood attack datagram (Figure 2, **5.1 Example Network**, pages 5-6, **4 CenterTrack Design Issues**, pages 4-5, i.e. edge routers must be able to perform input debugging, **6.2 Hop-by-Hop Tracking**, i.e. find the source of the attack); and,

a tracking router adjacent to the egress edge router, the tracking router being configured to perform the security diagnostic functions, the ingress edge router rerouting the DoS flood attack datagram to the tracking router as to permit identification of the ingress edge router,

wherein the tracking router forms an overlay tracking network with respect to the plurality of edge routers (**4.1 Tracking Adjacencies**, page 4, **4 CenterTrack Design Issues**, pages 4-5, i.e. tracking routers must be able to perform input debugging, **6.2 Hop-by-Hop Tracking**, i.e. find the source of the attack).

19. Regarding claim 22, Stone teaches wherein the overlay tracking network further comprises additional tracking routers (**5.6 Tracking System IGP and IBGP**, page 7, i.e. "tracking routers are fully meshed over tunnels").

20. Regarding claim 26, Stone teaches wherein the ingress edge router routes the DoS flood attack datagram to the tracking router due to a dynamic routing update from the tracking router (**5.2 Dynamic Routing with Tunnels**, page 6).

21. As per claim 28, Stone teaches a computer-readable medium carrying one or more sequences of one or more instructions for tracking denial-of-service floods (DoS), the one or more sequences of one or more instructions including instructions which, when executed by one or more processors, cause the one or more processors to perform the steps of:

receiving a DoS flood attack datagram on an overlay network formed by a tracking router (Abstract, page 1, i.e. "CenterTrack is an overlay network, consisting of IP tunnels, that is used to selectively reroute interesting datagrams directly from edge routers to special tracking routers.");

identifying the DoS flood attack datagram (Abstract, page 1, i.e. "the datagrams can be examined, then dropped or forwarded to the appropriate egress point");

identifying, by the tracking router, a previous hop router associated with the DoS flood attack datagram to determine an ingress adjacency associated with the DoS flood attack (**6.2 Hop-by-Hop Tracking**, page 8).

22. Regarding claim 29, Stone teaches wherein the computer readable medium further includes instructions for causing the one or more processors to perform the steps of: instructing the previous hop router to identify a respective previous hop router associated with the DoS flood attack datagram (**6.2 Hop-by-Hop Tracking**, page 8).

Conclusion

23. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

24. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

25. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christian LaForgia
Patent Examiner
Art Unit 2131

clf

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100